| # | LS |
|---|---|
| | |

HKUST – Department of Computer Science and Engineering
**COMP170: Discrete Math Tools for CS – FALL 2007**

# Midterm Examination 2

Sketch Solution Key

Date: Thursday, Nov 8, 2007 Time: 19:00–20:30 Venues: LTA, LTB

| | |
|---|---|
| Name: ____________________ | Student ID: ______________ |
| Email: ____________________ | Lecture and Tutorial: ________ |

**Instructions**

- This is a closed book exam. It consists of 20 pages and 8 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Only use notation given in class. Do not use notation that you have learnt outside of this class that is nonstandard.
- Calculators may be used for the exam.

| Questions | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Total |
|---|---|---|---|---|---|---|---|---|---|
| Points | 12 | 12 | 14 | 12 | 12 | 11 | 12 | 15 | 100 |
| Score | | | | | | | | | |

Student ID: ______________

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

> I declare that the answers submitted for this examination are my own work.
>
> I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.
>
> Student's Name: ______________________
>
> Student's Signature: ______________________

Student ID: ______________

Definitions and Formulas: This page contains some definitions used in this exam and a list of formulas (theorems) that you may use in the exam (without having to provide a proof). Note that you might not need all of these formulas on this exam.

Definitions

1. $N = \{0, 1, 2, 3, \ldots\}$, the set of non-negative integers.
2. $Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers.
3. $Z$ is the set of *all* integers.
4. $R$ is the set of *real numbers.*
5. $R^+$ is the set of positive *real numbers.*

Formulas:

1. $\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$
2. If $0 < i < n$ then $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$
3. $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$
4. $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$
5. $p \Rightarrow q$ is equivalent to $\neg p \vee q$
6. $\neg \forall x \in U\,(p(x))$ is equivalent to $\exists x \in U\,(\neg p(x))$
7. $\sum_{i=1}^{n-1} i = n(n-1)/2$
8. $\sum_{i=1}^{n-1} i^2 = \frac{2n^3 - 3n^2 + n}{6}$
9. If $r \neq 1$ then $\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$
10. If $r \neq 1$ then $\sum_{i=0}^{n} ir^i = \frac{nr^{n+2} - (n+1)r^{n+1} + r}{(1-r)^2}$

Student ID: ______________

**Problem 1:** [12 pts]

Recall the RSA public key cryptography scheme. Bob posts a public key $P = (n, e)$ and keeps a secret key $S = (n, d)$. When Alice wants to send a message $0 < M < n$ to Bob, she calculates $M' = M^e \bmod n$ and sends $M'$ to Bob. Bob then decrypts this by calculating $(M')^d \bmod n$. In class we learnt that in order for this scheme to work, $n, e, d$ must have special properties.
*(Note: In real life, to ensure a high level of security, $n, e, d$ have to be very large numbers. For simplicity, however, we do not consider that fact here and use small numbers in this question.)*

For each of the three Public/Secret ($P/S$) key pairs listed below:
(i) say whether it is a valid set of RSA Public/Secret key pairs and
(ii) justify your answer.

(a) $P = (91, 25)$, $S = (91, 51)$

(b) $P = (91, 25)$, $S = (91, 49)$

(c) $P = (84, 25)$, $S = (84, 37)$

**Solution:** Recall that the conditions for a pair to be correct is that
(i) $n = pq$ where $p$ and $q$ are prime numbers and
(ii) $e \cdot d \bmod T = 1$ where $T = (p-1)(q-1)$.

(a) This is not a valid key pair. It is true that $n = 7 \cdot 13$ so $p, q$ are prime. But $T = 72$ and $25 \cdot 51 \bmod 72 \neq 1$.

Note: It is also true that $25 \cdot 51 \bmod 91 = 1$ but that is not the RSA condition.

(b) This is a valid key pair since $n = 7 \cdot 13$ and $25 \cdot 49 \bmod 72 = 1$.

(c) This is not a valid key pair since $n = 7 \cdot 12$ and 12 is not prime.

Note: It is true that $e \cdot d \bmod n = 1$ and $e \cdot d \bmod (6 \cdot 11) = 1$ but this doesn't mean anything.

**Problem 2:** [12 pts]

Calculate the value of

$$3^{1032} \bmod 50.$$

Show the steps to obtain the result.

**Solution:** Use repeated squaring to calculate

$$\begin{aligned}
3^1 \bmod 50 &= 3 \\
3^2 \bmod 50 &= 9 \\
3^4 \bmod 50 &= 9^2 \bmod 50 = 31 \\
3^8 \bmod 50 &= 31^2 \bmod 50 = 11 \\
3^{16} \bmod 50 &= 11^2 \bmod 50 = 21 \\
3^{32} \bmod 50 &= 21^2 \bmod 50 = 41 \\
3^{64} \bmod 50 &= 41^2 \bmod 50 = 31 \\
3^{128} \bmod 50 &= 31^2 \bmod 50 = 11 \\
3^{256} \bmod 50 &= 11^2 \bmod 50 = 21 \\
3^{512} \bmod 50 &= 21^2 \bmod 50 = 41 \\
3^{1024} \bmod 50 &= 41^2 \bmod 50 = 31
\end{aligned}$$

Then

$$\begin{aligned}
3^{1032} \bmod 50 &= \left(3^{1024} \bmod 50\right) \cdot \left(3^8 \bmod 50\right) \bmod 50 \\
&= 31 \cdot 11 \bmod 50 \\
&= 41
\end{aligned}$$

Note: Fermat's little theorem could not be used to solve this problem because "50" is not prime.

Student ID: ____________

**Problem 3:** [14 pts]

Consider the following two sets of modular equations:

(a)

$$\begin{aligned} x \bmod 36 &= 12 \\ x \bmod 51 &= 5 \end{aligned}$$

(b)

$$\begin{aligned} x \bmod 35 &= 12 \\ x \bmod 69 &= 5 \end{aligned}$$

For each of the two sets of equations answer the following question:

> Does there exist a unique solution for $x \in Z_{mn}$, where $m$ and $n$ are the divisors of the two modular equations?

Note: in (a), $(m, n) = (36, 51)$; in (b), $(m, n) = (35, 69)$.

For each set, explain why your answer is correct. Furthermore, if your answer is that there is a unique solution, give the solution.

**Solution:**

(i) There is no solution.

The proof is by contradiction. Suppose that there is a solution $x$ in $Z_{mn}$.

Consider the first equation: $x \bmod 36 = 12$. Since both 36 and 12 are divisible by 3, we must have that $x$ is divisible by 3.

But, since 51 is also divisble by 3, this implies that $x \bmod 51$ is also divisible by 3. This contradicts the fact that 5 is not divisible by 3.

Note: The fact that $gcd(36, 51) \neq 1$ and therefore the Chinese Remainder Theorem can not be applied is not a valid solution to the problem. When the CRT can be applied, it tells us that there is a unique solution to the equalities. But, the fact that the CRT can not be applied, tells us nothing about the solutions (or lack of them).

(ii) Since $m = 35$ and $b = 69$ are relatively prime, the Chinese remainder theorem gurantees that there is a unique solution.

To find $x$ we first need to find $\bar{n} \in Z_m$ and $\bar{m} \in Z_n$ such that

$$n \cdot \bar{n} \bmod m = 1 \quad \text{and} \quad m \cdot \bar{m} \bmod n = 1.$$

It is easy to see (either by observation, or using the extended GCD algorithm) that

$$2 \cdot 35 + (-1) \cdot 69 = 1.$$

Thus $\bar{m} = 2$ and $\bar{n} = (-1) \bmod 35 = 34$.
Now let

$$y = 5 \cdot \bar{m} \cdot m + 12 \cdot \bar{n} \cdot n = 28502$$

and

$$x = y \bmod (mn) = 28502 \bmod 2415 = 1937.$$

Then, 1937 is the unique solution.

Student ID: ____________

**Problem 4:** [12 pts]

For each of the following pair of logical statements, either
(i) prove (using the inference rules discussed in class but *not* a truth table) that the two statements are logically equivalent, or
(ii) give a counterexample to show that the statements are not logically equivalent.

A counterexample for (a) and (b) would be a truth setting of the variables. A counterexample for (c) would be some universe $U$ and statements $p(x, y)$ and $q(x, z)$.

(a)

$$\begin{array}{rl} (i) & p \Rightarrow (q \Rightarrow r) \\ (ii) & (p \Rightarrow q) \Rightarrow r \end{array}$$

(b)

$$\begin{array}{rl} (i) & (p \wedge q) \Rightarrow (\neg(p \wedge r) \vee s) \\ (ii) & (p \wedge r) \Rightarrow ((p \wedge q) \Rightarrow s) \end{array}$$

(c)

$$\begin{array}{rl} (i) & \forall x \in U \ \neg\Big[(\exists y \in U \ p(x, y)) \wedge (\exists z \in U \ q(x, z))\Big] \\ (ii) & \forall x \in U \ (\forall y \in U \ \neg p(x, y)) \vee (\forall z \in U \ \neg q(x, z)) \end{array}$$

**Solution:** (a) They are not logically equivalent.
For example, when $p = F$, $q = T$ and $r = F$, (i) is True and (ii) is False.

(b) They are logically equivalent.

$$\begin{array}{rcll} (p \wedge q) \Rightarrow (\neg(p \wedge r) \vee s) & \equiv & \neg(p \wedge q) \vee (\neg(p \wedge r) \vee s) & (A \Rightarrow B) \equiv (\neg A \vee B) \\ & \equiv & (\neg(p \wedge q) \vee s) \vee \neg(p \wedge r) & \text{associative/commutative laws} \\ & \equiv & ((p \wedge q) \Rightarrow s) \vee \neg(p \wedge r) & (A \Rightarrow B) \equiv (\neg A \vee B) \\ & \equiv & (p \wedge r) \Rightarrow ((p \wedge q) \Rightarrow s) & (A \Rightarrow B) \equiv (\neg A \vee B) \end{array}$$

(c) They are logically equivalent. By the principles learnt in class for negating quantifiers we have

$$\begin{array}{rcl} \exists y \in U \ p(x, y) & \equiv & \neg\forall y \in U \neg p(x, y) \\ \exists z \in U \ q(x, z) & \equiv & \neg\forall z \in U \neg q(x, z) \end{array}$$

Therefore

$$\forall x \in U \ \neg\Big[(\exists y \in U \ p(x, y)) \wedge (\exists z \in U \ q(x, z))\Big] \equiv \forall x \in U \ \neg\Big[\neg\forall y \in U \neg p(x, y) \wedge \neg\forall z \in U \neg q(x, z)\Big]$$

which by De Morgan's law $\neg(\neg A \wedge \neg B) \equiv A \vee B$ is equivalent to

$$\forall x \in U \ (\forall y \in U \ \neg p(x, y)) \vee (\forall z \in U \ \neg q(x, z))$$

**Problem 5:** [12 pts]

Construct a contrapositive proof to show that:

If $n$ is a positive integer such that $n \bmod 3 = 2$,
then $n$ is not a perfect square.

*Note: Recall that $n$ is a perfect square if $n = k^2$ for some integer $k$.*

**Solution:** Let $p(n)$ and $q(n)$ denote the following two sentences:

$$p(n) \;:\; \text{`}n \text{ is a positive integer such that } n \bmod 3 = 2\text{'}$$
$$q(n) \;:\; \text{`}n \text{ is not a perfect square'}$$

The result that we need to prove can be expressed as the conditional statement $p(n) \Rightarrow q(n)$. A contrapositive proof corresponds to proving that $\neg q(n) \Rightarrow \neg p(n)$.

We first assume that $q(n)$ is false, i.e., $n$ is a perfect square or, equivalently, there exists some positive integer $k$ such that

$$n = k^2.$$

There are three cases to consider:

(i) If $k \bmod 3 = 0$, then $k = 3q$ for some integer $q$.
Then, $n = k^2 = 9q^2 = 3(3q^2)$. So $n \bmod 3 = 0$.

(ii) If $k \bmod 3 = 1$, then $k = 3q + 1$ for some integer $q$.
Then, $n = k^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. So $n \bmod 3 = 1$.

(iii) If $k \bmod 3 = 2$, then $k = 3q + 2$ for some integer $q$.
Then, $n = k^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$. So $n \bmod 4 = 1$.

For all three cases, $n \bmod 3$ is equal to 0 or 1, i.e., $p(n)$ is false. Thus we have $\neg q(n) \Rightarrow \neg p(n)$.

By the contrapositive rule of inference, we can conclude that $p(n) \Rightarrow q(n)$.

**Problem 6:** [11 pts]

For which values of $n \in N$ is the statement

$$2^{n-1} - 3 < 3^{n-3}$$

true? Prove the correctness of your answer.

**Solution:** It is true for $n = 0, 1, 2$ and all $n \geq 7$. It is not true for $n = 3, 4, 5, 6$.

One way to prove this is to first individually prove the statement is true or false for $n \leq 7$ and then prove by induction that, for all $n > 7$, the statement is true.

For the proof by induction you start with the fact that you have already seen the base case ($n = 7$) and then make the inductive hypothesis that the statement is true for $n = i - 1$, i.e.,

$$2^{(i-1)-1} - 3 < 3^{(i-1)-3}$$

or

$$2^{i-2} - 3 < 3^{i-4}$$

From this we get that

$$2^{i-1} - 6 = 2 \cdot \left(2^{i-2} - 3\right) < 2 \cdot 3^{i-4}$$

so

$$2^{i-1} - 3 < 2 \cdot 3^{i-4} + 3 < 2 \cdot 3^{i-4} + 3^{i-4} = 3^{i-3}.$$

That is, if $n > 7$ then the statement being true for $n = i - 1$ implies that the statement is true for $n = i$. Thus, by the principle of mathematical (weak) induction, the statement is true for all $n \geq 7$.

Note that in the second inequality we are assuming that "$3 < 3^{i-4}$." This is true because our original requirement was that $n \geq 7$ (and the statement is correct for $n > 5$.).

Student ID: ____________

**Problem 7:** [12 pts]

Consider $T(n)$ defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 5T(n-1) + 2n5^n & \text{if } n > 0 \end{cases}$$

(a) Give a closed-form solution for $T(n)$. It is not necessary to show how you derived your solution.

Also, your solution should *not* contain the summation sign ($\Sigma$) or "$\cdots$". As an example, you should not write something like "$\sum_{i=0}^{n-1} 2^i$" or "$1+2+\cdots 2^{n-1}$" in your solution. Instead, you should write "$2^n - 1$".

(b) Prove the correctness of your solution by induction.

**Solution:** (a)

$$T(n) = 5^n + 5^n n(n+1) = 5^n(n^2 + n + 1) \tag{1}$$

(b) The base case $n = 0$ follows by observation since

$$1 = 5^0(0^2 + 0 + 1).$$

Now assume that, for $n > 0$, equation (1) is correct for $n - 1$, i.e,

$$T(n-1) = 5^{n-1}((n-1)^2 + (n-1) + 1).$$

Plugging back into the defining equation gives

$$\begin{aligned} T(n) &= 5T(n-1) + 2n5^n \\ &= 5 \cdot 5^{n-1}(n^2 - n + 1) + 2n5^n \\ &= 5^n(n^2 + n + 1). \end{aligned}$$

Thus, (1) follows from the principle of weak induction.

Student ID: ____________

**Problem 8:** [15 pts]

Consider the recurrence relation defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 1 \\ a\,T(n/3) + n & \text{if } n > 1 \end{cases}$$

(a) Give a closed-form solution to $T(n)$ when $a = 1$.

(b) Give a closed-form solution to $T(n)$ when $a = 3$.

(c) Give a closed-form solution to $T(n)$ when $a = 9$.

For all of the problems you must *show your derivation.* That is, you need to show how you derived your solution. It is not necessary, though, to prove the correctness of your solution.

For all of the problems, you may always assume that $n$ is a power of 3. Also, your solution should *not* contain the summation sign ($\Sigma$) or "$\cdots$". As an example, you should not write something like "$\sum_{i=0}^{n-1} 2^i$" or "$1+2+\cdots 2^{n-1}$" in your solution. Instead, you should write "$2^n - 1$".

**Solution:** By iterating the recurrence, we derive that

$$T(n) = a^{\log_3 n} T(1) + n \sum_{i=0}^{(\log_3 n)-1} \left(\frac{a}{3}\right)^i.$$

Recalling that $T(1) = 1$ and

$$a^{\log_3 n} = \left(3^{\log_3 a}\right)^{\log_3 n} = n^{\log_3 a}$$

gives

$$T(n) = n^{\log_3 a} + n \sum_{i=0}^{(\log_3 n)-1} \left(\frac{a}{3}\right)^i \tag{2}$$

(a) Plugging $a = 1$ into (2) gives

$$\begin{aligned} T(n) &= n^{\log_3 1} + n \sum_{i=0}^{(\log_3 n)-1} \left(\frac{1}{3}\right)^i \\ &= n^0 + n\frac{1-(1/3)^{\log_3 n}}{1-\frac{1}{3}} \\ &= 1 + \frac{3n}{2}\left(1 - \frac{1}{n}\right) \\ &= \frac{3n}{2} - \frac{1}{2} \end{aligned}$$

(b) Plugging $a = 3$ into (2) gives

$$\begin{aligned} T(n) &= n^{\log_3 3} + n \sum_{i=0}^{(\log_3 n)-1} \left(\frac{3}{3}\right)^i \\ &= n + n \log_3 n \end{aligned}$$

(c) Plugging $a = 9$ into (2) gives

$$\begin{aligned} T(n) &= n^{\log_3 9} + n \sum_{i=0}^{(\log_3 n)-1} \left(\frac{9}{3}\right)^i \\ &= n^2 + n \frac{3^{\log_3 n} - 1}{3 - 1} \\ &= n^2 + n \frac{n - 1}{2} \\ &= \frac{3n^2 - n}{2}. \end{aligned}$$